

Multi-Prover Quantum Merlin-Arthur Proof Systems with Small Gap

Attila Pereszlényi*

Centre for Quantum Technologies, National University of Singapore

May 11, 2012

Abstract

This paper studies multiple-proof quantum Merlin-Arthur (QMA) proof systems in the setting when the completeness-soundness gap is small. Small means that we only lower-bound the gap with an inverse-exponential function of the input length, or with an even smaller function. Using the protocol of Blier and Tapp [BT09], we show that in this case the proof system has the same expressive power as non-deterministic exponential time (NEXP). Since single-proof QMA proof systems, with the same bound on the gap, have expressive power at most exponential time (EXP), we get a separation between single and multi-prover proof systems in the ‘small-gap setting’, under the assumption that $\text{EXP} \neq \text{NEXP}$. This implies, among others, the nonexistence of certain operators called disentanglers (defined by Aaronson et al. [ABD⁺09]), with good approximation parameters.

We also show that in this setting the proof system has the same expressive power if we restrict the verifier to be able to perform only Bell-measurements, i.e., using a BellQMA verifier. This is not known to hold in the usual setting, when the gap is bounded by an inverse-polynomial function of the input length. To show this we use the protocol of Chen and Drucker [CD10]. The only caveat here is that we need at least a linear amount of proofs to achieve the power of NEXP, while in the previous setting two proofs were enough.

We also study the case when the proof-lengths are only logarithmic in the input length and observe that in some cases the expressive power decreases. However, we show that it doesn’t decrease further if we make the proof lengths to be even shorter.

1 Introduction

Arthur-Merlin games and the class MA was defined by Babai [Bab85] as natural extension of the class NP using randomization. In the definition of MA the prover (Merlin) gives a polynomial length ‘proof’ to the verifier (Arthur), who then performs a polynomial-time randomized computation and has to decide if an input x is in a language or not. The verifier is allowed to make some error in the decision, hence making the class MA possibly more powerful than NP. If we add communication to the model, i.e., the prover and the verifier can exchange a polynomial number of messages then we get the class IP [GMR89].¹ The classes IP and MA has been extensively studied and it is known that in both cases we can make the protocol to have one-sided, exponentially small error without hurting the power of the proof system. I.e., the verifier only makes an error if the input is not in the language, and even in this case the error probability is at most an inverse-exponential function of the input length. Surprisingly, it turned out that IP is equal to the class of problems decidable in polynomial space (PSPACE) [LFKN92, Sha92]. For more information on these classes see e.g., the book of Arora and Barak [AB09].

*E-mail: attila.pereszlényi@gmail.com.

¹Babai also defined an interactive version of MA, that can be thought of as a ‘public-coin’ version of IP. Later Goldwasser and Sipser [GS86] showed that this class has the same expressive power as IP.

Quantum Merlin-Arthur proof systems (and the class QMA) were introduced by Knill [Kni96], Kitaev [KSV02], and also by Watrous [Wat00] as a natural extension of MA and NP to the quantum computational setting. Similarly, quantum interactive proof systems (and the class QIP) were introduced by Watrous [Wat03] as a quantum analogue of IP. These classes have also been well studied and now it's known that the power of quantum interactive proof systems is the same as the classical ones, i.e., $\text{QIP} = \text{IP} = \text{PSPACE}$ [JJUW10]. Furthermore, quantum interactive proof systems still have the same expressive power if we restrict the number of messages to three and have exponentially small one-sided error [KW00]. The class QMA can also be made to have exponentially small error, and has natural complete problems [AN02]. Interestingly it's not known if we can make QMA to have one-sided error.²

Several variants of QIP and QMA have also been studied. For example one can consider the case where some or all of the messages are short, meaning at most logarithmic in the input length [MW05, BSW11, Per11]. Our focus will be more on the setting that was introduced by Ito, Kobayashi and Watrous [IKW10]. They studied quantum classes where the gap between the completeness and soundness parameter is very small. Their main result is that quantum interactive proofs with double-exponentially small gap is characterized by EXP (deterministic exponential time).

Probably the most interesting generalization of QMA is by Kobayashi, Matsumoto and Yamakami [KMY03] who defined the class $\text{QMA}[k]$. In this setting there are k provers who send k quantum proofs to the verifier, and these proofs are guaranteed to be unentangled. Note that in the classical setting this generalization is not interesting since we can just concatenate the k proofs and treat them as one proof. However, in the quantum case a single prover can entangle the k proofs and no method is known to detect such a cheating behavior.

Obviously the most important question is whether more provers make the class more powerful or not. In a later version of their paper, Kobayashi et al. [KMY03] (and independently Aaronson et al. [ABD⁺09]) showed that $\text{QMA}[2] = \text{QMA}[k]$ for all polynomially-bounded k if and only if $\text{QMA}[2]$ can be amplified to exponentially small error. Later Harrow and Montanaro [HM10] showed that the above equality indeed holds. The question now is whether QMA is equal to $\text{QMA}[2]$, or in other words, does unentanglement actually help? There are signs that show that the above two classes are probably not equal. For example, Liu, Christandl, and Verstraete [LCV07] found a problem that has a $\text{QMA}[2]$ proof system, but not known to belong to QMA. Blier and Tapp [BT09] showed that all problems in NP have a $\text{QMA}[2]$ proof system where the length of both proofs are logarithmic in the input length. On the other hand, if QMA has one logarithmic-length proof then it has the same expressive power as BQP [MW05]. Since BQP is not believed to contain NP, $\text{QMA}[2]$ with logarithmic length proofs is probably more powerful than QMA with a logarithmic proof. The above proof system had some inverse-polynomial gap, and this gap was later improved by several papers [Bei10, CF11, GNN11]. However, in all of these improvements the gap is still an inverse-polynomial function of the input length.³ Another evidence is by Aaronson et al. [ABD⁺09] who found a $\text{QMA}[\tilde{O}(\sqrt{n})]$ proof system for 3SAT with constant gap and where each proof consist of $O(\log n)$ qubits. Again, it seems unlikely that 3SAT has a proof system with one $\tilde{O}(\sqrt{n})$ -length proof.

1.1 Our Contribution

We study multiple-proof QMA proof systems in the setting where the completeness-soundness gap is exponentially small or even smaller. We examine three variants of these proof systems as described below.

²In a recent paper, Jordan et al. [JKNN11] showed that the proof system can achieve perfect completeness if the prover's message is classical.

³It is not believed that the gap in this setting can be improved to a constant because it would imply that $\text{QMA}[2] = \text{NEXP}$. [ABD⁺09]

1.1.1 QMA $[k]$ with Small Gap

The first variant we look at is the small-gap version of QMA $[k]$ mentioned above. We show that this class is exactly characterized by NEXP if the number of proofs are between 2 and $\text{poly}(n)$, and the completeness-soundness gap is between exponentially or double-exponentially small. The power of the proof system is still NEXP if we require it to have one-sided error. More precisely we show the following theorem.

Theorem 1.1. $\text{NEXP} = \text{QMA}(\text{poly}, 2, 1, 1 - \Omega(4^{-n})) = \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(\text{poly}, \text{poly}, c, s)$, where $c(n)$

and $s(n)$ can be calculated in time at most exponential in n on a classical computer.

In the notation above the first parameter of QMA is the upper-bound on the length of each proofs the verifier receives, in qubits. The second parameter denotes the number of unentangled proofs, while the third is the completeness and the fourth is the soundness parameter. For a precise definition of the above notation see Section 2. Note that in Theorem 1.1 the NEXP upper-bound is trivial, as it follows from exactly the same argument that shows the NEXP upper-bound to the ‘normal-gap’ QMA[2]. Interestingly, there is no other upper-bound known for QMA[2], and it is a big open question to strengthen this bound [ABD⁺09]. The surprising phenomenon is that if we relax the bound on the gap, then the expressive power of the class jumps all the way up to the trivial upper-bound. Note that an EXP upper-bound for the small-gap, single-prover QMA is easily seen, so we have a separation between QMA and QMA $[k]$ in the small-gap setting. For more discussion about this and other consequences see Section 5.

The non-trivial part of the proof is proving the NEXP lower-bound. For this we use the protocol of Blier and Tapp [BT09] on a NEXP-complete language which we call SUCCINCT3COL, the succinct version of graph 3-coloring. The proof of Theorem 1.1 is presented in Section 3.

1.1.2 BellQMA $[k]$ with Small Gap

The class BellQMA $[k]$ was defined by Aaronson et al. [ABD⁺09], Brandão [Ba08], and Chen and Drucker [CD10]. The above definitions are not exactly the same, but the subtle difference doesn’t matter in either of the above papers, neither it does in this paper. The exact definition of the class can be found in Section 2. Roughly, the difference between QMA $[k]$ and BellQMA $[k]$ is that in the latter the verifier has to measure each proof separately and non-adaptively, then based on the outcomes has to make its decision. Aaronson et al. [ABD⁺09] asked the question whether BellQMA $[k]$ has the same power as QMA $[k]$ and if there is a BellQMA protocol for 3SAT with similar parameters as theirs. A partial positive answer to the first question was given by Brandão [Ba08], who showed that $\text{BellQMA}[O(1)] = \text{QMA}$, and a positive answer to the second question was given by Chen and Drucker [CD10]. The power of BellQMA $[k]$ with super-constant k remains an open problem.

In this paper we study the small-gap version of BellQMA $[k]$, where again small means exponentially or double-exponentially small. One can observe that Brandão’s proof of $\text{BellQMA}[O(1)] = \text{QMA}$ doesn’t go through if the gap is so small.⁴ So we don’t know the power of BellQMA $[k]$ with constant k in the small-gap setting. However, we show that if $k = \Omega(n)$ then BellQMA $[k]$ has the same power as QMA $[k]$, i.e., it also equals to NEXP. This is expressed by the following theorem.

Theorem 1.2. $\text{NEXP} = \text{BellQMA}(\text{poly}, \Omega(n), c, s) = \bigcup_{\substack{0 < s' < c' \leq 1, \\ c'-s' \geq 2^{-2^{\text{poly}}}}} \text{BellQMA}(\text{poly}, \text{poly}, c', s')$, for some c

and s with $c(n) - s(n) = \Omega(4^{-n})$, and where $c'(n)$ and $s'(n)$ can be calculated in time at most exponential in n on a classical computer.

⁴Aaronson et al. [ABD⁺09] also defined the class LOCCQMA similarly to BellQMA but allowing the verifier to make adaptive and even several measurements on the same proofs. Brandão, Christandl, and Yard [BaCY11] showed that $\text{LOCCQMA}[O(1)] = \text{QMA}$. This proof also breaks down if the gap is small.

In the above the NEXP upper-bound is again trivial, so the only thing we need to do is give a BellQMA protocol for NEXP. Just as in the proof of the previous theorem, we will use the same language (SUCCINCT3COL) and give a proof system for that. For this we will use the protocol of Chen and Drucker [CD10]. Note that similarly to their original protocol we don't have perfect completeness either.

Knowing that having sufficiently many provers makes BellQMA[k] as powerful as QMA[k], it would be very interesting to know the power of BellQMA[k] with small gap and constant k . It's either more powerful than BellQMA[1] = QMA, or somewhere between constant and linear number of provers there is an increase in the expressive power. A more detailed discussion about this can be found in Section 5.4, and the proof of Theorem 1.2 is presented in Section 4.

1.1.3 QMA[k] with Small Gap and Short Proofs

We also study the small-gap version of QMA[k] where each proof is short i.e., at most $O(\log n)$ -many qubits. One would expect that in this case the class gets weaker than NEXP. We could only show this in the case when the gap is inverse-exponential, which follows from a few simple observations. For the case when the gap is smaller than this we give a lemma that simplifies the proof system, which may help to prove non-trivial upper-bounds for these classes later. The lemma roughly says that instead of $O(\log n)$ -many qubits, we can consider the case when all the proof are just 1 qubits. The above mentioned results are described in more detail in Section 5.6.

Organization of the Paper

The remainder of the paper is organized as follows. Section 2 discusses the background theorems and definitions needed for the rest of the paper. Section 3 presents the proof of our first main theorem, Theorem 1.1, with the last part of the proof presented in Appendix A. In Section 4 we explain the proof of our other main theorem, Theorem 1.2. We end the paper with some conclusions and open problems in Section 5, with one last proof presented in Appendix B.

2 Preliminaries

We assume familiarity with quantum information and computation [NC00]; such as quantum states, unitary operators, measurements, etc. We also assume the reader is familiar with computational complexity, both classical [AB09] and quantum [Wat08]. Throughout the paper we will talk about complexity classes like PP, PSPACE, EXP, NEXP, BQP, PQP, QMA, and QIP. In this section we only define the classes that are the most relevant to our discussions, where the definition of the rest can be found in the above mentioned references. The purpose of this section is to present some of the notations and background information (definitions, theorems) required to understand the rest of the paper.

We denote the set of functions of n that are upper-bounded by some polynomial in n by $\text{poly}(n)$. If the argument is clear, we omit it and just write poly . We denote the imaginary unit by ι instead of i , which we use as an index in summations for example.

Definition 2.1. In the paper we use some well-known quantum gates. We define them here.

$$\begin{aligned}\text{CNOT} &\stackrel{\text{def}}{=} |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\ \mathbf{H} &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \\ \mathbf{R}_x(\omega) &\stackrel{\text{def}}{=} \cos \frac{\omega}{2} |0\rangle\langle 0| - \iota \sin \frac{\omega}{2} |0\rangle\langle 1| - \iota \sin \frac{\omega}{2} |1\rangle\langle 0| + \cos \frac{\omega}{2} |1\rangle\langle 1| \\ \mathbf{R}_z(\omega) &\stackrel{\text{def}}{=} |0\rangle\langle 0| + e^{\iota\omega} |1\rangle\langle 1|\end{aligned}$$

Whenever we talk about quantum polynomial-time algorithms or quantum verifiers, we always mean polynomial-time uniformly generated quantum circuits consisting of some universal set of gates. For example, the gates **CNOT**, **H**, and $\mathbf{R}_z(\frac{\pi}{4})$ form a universal set, and there are many other sets that are universal. Usually it doesn't matter which set we choose when we define quantum verifiers and classes like QMA and QIP, because it is known that each universal set can approximate any other set with exponential precision. However, in the following we will use error parameters that are smaller than this, hence the power of those classes may change with respect to what set of gates the verifier is using. In this paper we only assume that the verifier can perform or perfectly simulate the **CNOT** and the **H** gate, besides being able to perform any polynomial-time classical computation. This assumption is enough for all our results, so we won't bother about the gate set in the rest of the paper.

Definition 2.2 ([KMY03, ABD⁺09]). For functions $\ell, k : \mathbb{Z}^+ \rightarrow \mathbb{N}$, $c, s : \mathbb{Z}^+ \rightarrow (0, 1]$ a language L is in $\text{QMA}(\ell, k, c, s)$ if there exist a quantum verifier V such that for all $n \in \mathbb{Z}^+$ and inputs $x \in \{0, 1\}^n$, $V(x)$ is a quantum circuit generated in $\text{poly}(n)$ -time and the following holds.

Completeness: If $x \in L$ then there exist quantum proofs $|\phi_1\rangle, \dots, |\phi_{k(n)}\rangle$, where for all i , $|\phi_i\rangle$ is made up of at most $\ell(n)$ qubits, and the acceptance probability of $V(x)$ on input $|\phi_1\rangle \otimes \dots \otimes |\phi_{k(n)}\rangle$ is $\geq c(n)$.

Soundness: If $x \notin L$ then for all states $|\phi_1\rangle, \dots, |\phi_{k(n)}\rangle$, where for all i , $|\phi_i\rangle$ is made up of at most $\ell(n)$ qubits, $V(x)$ accepts with probability $\leq s$, given $|\phi_1\rangle \otimes \dots \otimes |\phi_{k(n)}\rangle$ as its input.

If the class is denoted by $\text{QMA}(\ell, k, c, < s)$, then the probability bound in the soundness case is $< s$ instead of $\leq s$.

Remark 2.3. If we just give one parameter to QMA, then it indicates the number of provers. So the notation $\text{QMA}[k]$ is defined as $\text{QMA}[k] \stackrel{\text{def}}{=} \text{QMA}(\text{poly}(n), k, \frac{2}{3}, \frac{1}{3})$. With our notation the class QMA is defined as $\text{QMA} \stackrel{\text{def}}{=} \text{QMA}[1]$.

Definition 2.4 ([Ba08, ABD⁺09]). The class $\text{BellQMA}(\ell, k, c, s)$ is defined almost the same way as $\text{QMA}(\ell, k, c, s)$ in Definition 2.2, except that the verifier V is not an arbitrary poly-time quantum computation. The restriction we put on the verifier is the following. V upon seeing x performs a classical randomized poly-time computation and produces circuits for measurements $M_1, \dots, M_{k(n)}$, where each M_i is a POVM on at most $\ell(n)$ qubits. Then for all i , the verifier measures $|\phi_i\rangle$ with M_i , and obtains outcome m_i . After all measurements were performed, V runs a classical computation on inputs $m_1, \dots, m_{k(n)}$, and decides whether to accept or reject.

Note that in the above definition the verifier has to measure each proofs separately. Moreover, none of the circuits of the measurements can depend on the outcome of any previous measurement. Chen and Drucker [CD10] defined BellQMA in a slightly different way by allowing the verifier to do quantum computations before and after the measurements. Our result also holds if we take their definition. The reason we chose the above definition is because we will prove a lower-bound for our BellQMA class, and so with the more restricted definition our result is slightly stronger.

Definition 2.5. The class $\text{QCMA}(c, s)$ is defined analogously to QMA of Definition 2.2 with the difference that the proof must be a classical string. We will always take this string to be polynomial-length. Since the string is classical, it doesn't make sense to have several proofs, so we drop the parameters of proof lengths and number of proofs. As in the previous definitions, c is the completeness and s is the soundness parameter.

Definition 2.6 ([GW83]). Let $G(V, E)$ be an undirected graph where $V = \{0, 1, \dots, m-1\}$ and $m \leq 2^n$ for some n . We define C_G to be a *small circuit representation* of G if the following hold:

- C_G is a circuit containing AND, OR and NOT gates.
- C_G has two inputs of n bits each.
- C_G has $\text{poly}(n)$ gates.
- The output of C_G is given by

$$C_G(u, v) = \begin{cases} 00 & \text{if } u \notin V \text{ or } v \notin V \text{ or } u \geq v, \\ 10 & \text{if } u < v \text{ and } (u, v) \notin E, \\ 11 & \text{if } u < v \text{ and } (u, v) \in E. \end{cases}$$

Definition 2.7. Let the decision problem **SUCCINCT3COL** be the set of small circuit representations of graphs that are 3-colorable.

Theorem 2.8 ([PY86]). **SUCCINCT3COL** is NEXP-complete.

In the following discussion we will use the ‘SWAP-test’ of [BAD⁺97, BCWdW01], and the following property of this test.

Theorem 2.9 ([BCWdW01]). When the SWAP-test is applied to two states $|\varphi\rangle$ and $|\psi\rangle$ (with the same dimension), it accepts with probability $\frac{1}{2} (1 + |\langle\varphi|\psi\rangle|^2)$.

Note that in order to perform the SWAP-test we need two Hadamard (**H**) gates, **CNOT** gates with the amount linear in the number of qubits $|\varphi\rangle$ and $|\psi\rangle$ are stored on, and we need to measure a qubit in the standard basis.

Definition 2.10. We define the state $|u_m\rangle$ as the uniform superposition of the standard basis states, i.e.,

$$|u_m\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle.$$

We also define the projective measurement that projects onto this state, or more formally the measurement $\{\mathbf{P}_0, \mathbf{P}_1\}$ where

$$\mathbf{P}_0 \stackrel{\text{def}}{=} |u_m\rangle\langle u_m|, \quad \mathbf{P}_1 \stackrel{\text{def}}{=} \mathbb{1} - |u_m\rangle\langle u_m|.$$

We say that \mathbf{P}_0 (and \mathbf{P}_1) corresponds to outcome 0 (and 1).

Note that the above measurement can be performed using $\lceil \log m \rceil$ Hadamard gates and single-qubit measurements.

3 QMA $[k]$ with Small Gap Equals NEXP

This section proves Theorem 1.1, i.e., we show that QMA $[k]$ equals NEXP if k is at least 2 and at most $\text{poly}(n)$, and the completeness-soundness gap is bounded away by an inverse-exponential or doubly exponential function of n .

The proof of this theorem is divided into Lemma 3.1 and Theorem 3.2, according to the two directions of the containment. As mentioned in the Introduction, only Theorem 3.2 is actually new.

Lemma 3.1. $\bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(\text{poly}, \text{poly}, c, s) \subseteq \text{NEXP}$, where $c(n)$ and $s(n)$ can be calculated in time

at most exponential in n on a classical computer.

Proof sketch. Let $L \in \text{QMA}(\text{poly}, \text{poly}, c, s)$ with some c and s satisfying the conditions in the lemma. The proofs in the QMA proof system are poly-many quantum states on poly-many qubits, which are vectors in the complex euclidean space with exponential dimension. These vectors can be described up to an exponential number of bits of accuracy by a classical proof of exponential length. Given this proof to a NEXP machine, it can calculate the acceptance probability of the QMA verifier to an exponential number of bits of accuracy; and it can decide whether this probability is more than c or less than s . This means that $L \in \text{NEXP}$. \square

The other direction of the containment is formulated by the following theorem.

Theorem 3.2. $\text{NEXP} \subseteq \text{QMA}(\text{poly}, 2, 1, 1 - \Omega(4^{-n}))$.

We will prove this result through several lemmas. This will prove Theorem 1.1 as well.

Proof of Theorem 1.1. The theorem immediately follows from Lemma 3.1, Theorem 3.2 and the observation that $\text{QMA}(\text{poly}, 2, 1, 1 - \Omega(4^{-n})) \subseteq \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(\text{poly}, \text{poly}, c, s)$. \square

In order to prove Theorem 3.2 we construct a QMA verifier V for the NEXP-complete language **SUCCINCT3COL**. We use the protocol of Blier and Tapp [BT09], with similar argument as theirs.

Let the input to **SUCCINCT3COL** be denoted by C_G and its length by $n = |C_G|$. Let V get its two unentangled proofs in registers R_1 and R_2 . Both R_i 's have two parts, $R_i = N_i C_i$, where N_i is the 'node' part and C_i is the 'color' part. N_1 and N_2 have associated Hilbert space \mathbb{C}^{2^n} , while C_1 and C_2 have associated space \mathbb{C}^3 . The procedure V performs is described in Algorithm 1.

Algorithm 1 Description of verifier V in the proof of Theorem 3.2.

Input : classical circuit C_G , quantum registers R_1 and R_2 , where the state of R_1 and R_2 is separable

Output : accept or reject

- 1: With probability $1/3$ do the **Equality Test** (line 2), the **Consistency Test** (line 8), or the **Uniformity Test** (line 16).
 - 2: **Equality Test.** Perform the SWAP-test on R_1 and R_2 .
 - 3: **if** the SWAP-test fails **then**
 - 4: **return** reject *{The two registers are not equal.}*
 - 5: **else**
 - 6: **return** accept
 - 7: **end if**
 - 8: **Consistency Test.** Measure N_1 , C_1 , N_2 and C_2 in the computational basis and get v_1 , c_1 , v_2 and c_2 .
 - 9: **if** ($v_1 = v_2$) **and** ($c_1 \neq c_2$) **then**
 - 10: **return** reject *{The same vertex has two colors.}*
 - 11: **else if** ($C(v_1, v_2) = 11$) *{Assume that $v_1 < v_2$ otherwise swap them.}* **and** ($c_1 = c_2$) **then**
 - 12: **return** reject *{Adjacent vertices have same color.}*
 - 13: **else**
 - 14: **return** accept
 - 15: **end if**
 - 16: **Uniformity Test.** Measure N_1 and C_1 separately according to the measurement of Definition 2.10.
 - 17: **if** (the outcome on C_1 is 0) **and** (the outcome on N_1 is 1) **then**
 - 18: **return** reject *{Not all nodes are present.}*
 - 19: **else**
 - 20: **return** accept
 - 21: **end if**
-

Note that V runs in $\text{poly}(n)$ -time, because the SWAP-test, evaluating the circuit C_G , and performing the measurement of Definition 2.10 for $m = 2^n$ all can be performed in polynomial time. The following lemma, which is essentially the same as Theorem 2.4 of [BT09], proves completeness for V .

Lemma 3.3 (Completeness). *If $C_G \in \text{SUCCINCT3COL}$ then there exist a pair of proofs, with which V will accept with probability 1.*

Proof. For $i \in \{0, 1, \dots, m-1\}$ let $c(i) \in \{0, 1, 2\}$ be a valid coloring of the graph G , where m is the number of nodes. For $i \in \{m, \dots, 2^n-1\}$ let $c(i) = 0$. Let the state of both R_1 and R_2 be

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle |c(i)\rangle, \quad (1)$$

where $|i\rangle$ is on the node register (N) and $|c(i)\rangle$ is on the color register (C). From Theorem 2.9 it follows that the Equality Test succeeds with probability 1. Since c is a valid 3-coloring, the Consistency Test succeeds with probability 1 as well. To see the same for the Uniformity Test, let us calculate the resulting state after measuring 0 on C_1 in line 17 of Algorithm 1. Up to some normalization factor, the state is

$$(\mathbb{1} \otimes |u_3\rangle\langle u_3|) |\phi\rangle = \frac{1}{3\sqrt{2^n}} \left(\sum_{i=0}^{2^n-1} |i\rangle \right) \otimes \left(\sum_{k=0}^2 |k\rangle \right).$$

This means that the state of N_1 is $|u_{2^n}\rangle$, so the Uniformity Test always succeeds. \square

The proof of soundness is presented in Appendix A on page 15, because it closely follows the analysis of Blier and Tapp [BT09] and of Chiesa and Forbes [CF11], although with different parameters.

4 BellQMA $[\Omega(n)]$ with Small Gap Equals NEXP

In this section we prove Theorem 1.2, i.e., we show that QMA with exponentially small gap still equals to NEXP if we restrict the verifier to only be able to perform Bell-measurements. However, we will need at least $\Omega(n)$ proofs. We essentially use the algorithm of Chen and Drucker [CD10] on the succinct version of graph 3-coloring (SUCCINCT3COL). We also use one of their lemmas, but our proof will be simpler than theirs, because we don't aim for constant gap. We don't use the PCP theorem either. Note that in the previous section we already argued about the NEXP upper-bound on the QMA classes. The same argument applies here too. It's also easy to see that restricting the verifier can only make the power of the proof system weaker. So the only statement left to prove, in order to prove Theorem 1.2, is the following.

Theorem 4.1. $\text{NEXP} \subseteq \text{BellQMA}(\text{poly}(n), \Omega(n), c, s)$, for some c and s with $c(n) - s(n) = \Omega(4^{-n})$.

To prove Theorem 4.1, we construct a BellQMA verifier V for SUCCINCT3COL which will show that $\text{SUCCINCT3COL} \in \text{BellQMA}(\text{poly}(n), \Omega(n), c, s)$. Since SUCCINCT3COL is NEXP-complete, Theorem 4.1 will follow. Just as in the previous section, let the input to SUCCINCT3COL be denoted by C_G and its length by $n = |C_G|$. Verifier V will receive k quantum proofs in registers $N_1, C_1, \dots, N_k, C_k$, where for each $i \in \{1, 2, \dots, k\}$, the state of $N_i C_i$ is separable from the rest of the registers. The registers N_i have associated space \mathbb{C}^{2^n} and registers C_i have associated space \mathbb{C}^3 , similarly as in the previous section. The behavior of V is described in Algorithm 2. We split the proof of Theorem 4.1 into Lemma 4.2, which proves completeness for V and Lemma 4.5, which proves its soundness.

Lemma 4.2 (Completeness). *If $C_G \in \text{SUCCINCT3COL}$ then there exist quantum states on registers $N_1, C_1, \dots, N_k, C_k$, such that if they are input to V , defined by Algorithm 2, then V will accept with probability at least $1 - 2^{-\frac{k}{40}}$.*

Algorithm 2 Description of verifier V in the proof of Theorem 4.1.

Input: classical circuit C_G , quantum registers $N_1, C_1, \dots, N_k, C_k$, where $\forall i \in \{1, 2, \dots, k\}$, the state of $N_i C_i$ is separable from the rest of the registers

Output: accept or reject

```
1: With probability  $\frac{1}{2}$  do the Consistency Test (line 2) or the Uniformity Test (line 14).
2: Consistency Test.
3: for all  $i \in \{1, 2, \dots, k\}$  do
4:   Measure  $N_i$  and  $C_i$  in the computational basis and get  $v_i$  and  $c_i$ .
5: end for
6: for all  $1 \leq i < j \leq k$  do
7:   if  $(v_i = v_j)$  and  $(c_i \neq c_j)$  then
8:     return reject {The same vertex has two colors.}
9:   else if  $(C_G(v_i, v_j) = 11)$  and  $(c_i = c_j)$  then
10:    return reject {Adjacent vertices have same color.}
11:   end if
12: end for
13: return accept
14: Uniformity Test.
15: for all  $i \in \{1, 2, \dots, k\}$  do
16:   Measure  $C_i$  with the measurement of Definition 2.10 and denote the outcome by  $x_i$ .
17:   Measure  $N_i$  with the measurement of Definition 2.10 and denote the outcome by  $y_i$ .
18: end for
19: Let  $Z \stackrel{\text{def}}{=} \{i : x_i = 0\}$ .
20: if  $|Z| < k/6$  then
21:   return reject
22: end if
23: for all  $i \in Z$  do
24:   if  $y_i = 1$  then
25:     return reject {Not all nodes are present.}
26:   end if
27: end for
28: return accept
```

Proof. For all $i \in \{1, 2, \dots, k\}$, let the state of $N_i C_i$ be $|\phi\rangle$, where $|\phi\rangle$ is defined by equation (1) on page 8. For exactly the same reason as in the proof of Lemma 3.3 the Consistency Test will succeed with probability 1. As for the Uniformity Test, note that for all $i \in Z$, the measurement of N_i in line 17 of Algorithm 2 yields 1 with probability 1. The argument for this is also in the proof of Lemma 3.3.

This means that given the above input, the only place where Algorithm 2 may reject is at line 21, i.e., when $|Z| < \frac{k}{6}$. So in the following we only need to upper-bound this probability. We do it similarly to the proof of Lemma 1 of [CD10]. By direct calculation the probability that $x_i = 0$ in line 16 is

$$\Pr[x_i = 0] = \langle \phi | (\mathbb{1} \otimes |u_3\rangle\langle u_3|) | \phi \rangle = \frac{1}{3}.$$

This means that $\mathbb{E}[|Z|] = \frac{k}{3}$. Since the x_i 's are independent, we can use the Chernoff bound and get that

$$\Pr\left[|Z| < \frac{k}{6}\right] < e^{-\frac{k}{48}} < 2^{-\frac{k}{40}}.$$

This finishes the proof of the lemma. □

We are left to prove soundness for V . From now on let's denote the quantum input to Algorithm 2 by $|\varphi_1\rangle, \dots, |\varphi_k\rangle$. For each $i \in \{1, 2, \dots, k\}$, we write

$$|\varphi_i\rangle = \sum_{v=0}^{2^n-1} \alpha_v^{(i)} |v\rangle \sum_{j=0}^2 \beta_{v,j}^{(i)} |j\rangle,$$

where $|v\rangle$ is a state on N_i , $|j\rangle$ is a state on C_i , furthermore $\sum_{v=0}^{2^n-1} |\alpha_v^{(i)}|^2 = 1$ for each i , and $\sum_{j=0}^2 |\beta_{v,j}^{(i)}|^2 = 1$ for each i and v . Similarly to the notation in [CD10] let

$$Z' \stackrel{\text{def}}{=} \left\{ i : \Pr[x_i = 0] \geq \frac{1}{12} \right\}.$$

We need a lemma from [CD10] which we will state and use with a bit different parameters. Intuitively the lemma says that in order to avoid rejection in line 21, we must have a constant fraction of registers for which, with at least a constant probability, the outcome of the measurement in line 16 is 0.

Lemma 4.3 (Lemma 2 of [CD10]). *If $|Z'| \leq k/6$ and if in line 1 of Algorithm 2 the Uniformity Test is chosen, then the test will reject in line 21 with probability $\Omega(1)$.*

We want all nodes to appear with sufficiently big amplitude in $|\varphi_i\rangle$, for each $i \in Z'$. This is formalized by the following lemma.

Lemma 4.4. *Suppose that the Uniformity Test rejects with probability at most $200^{-1} \cdot 4^{-n}$. Then $\forall i \in Z'$ and $\forall v \in \{0, 1, \dots, 2^n - 1\}$ it holds that*

$$|\alpha_v^{(i)}|^2 > \frac{1}{24 \cdot 2^n}.$$

Proof. Let's pick an $i \in Z'$, and consider the state $|\varphi_i\rangle$ on register $N_i C_i$. Suppose that we measured 0 on C_i with the measurement of Definition 2.10, and denote the resulting state on N_i by

$$|\xi_i\rangle = \sum_{v=0}^{2^n-1} \gamma_v^{(i)} |v\rangle.$$

Note that since $i \in Z'$, this outcome happens with probability $\geq \frac{1}{12}$. Assume towards contradiction that $\exists v$ such that $|\gamma_v^{(i)}|^2 < \frac{1}{2 \cdot 2^n}$. Using Lemma A.4 from page 17, we get that when we measure $|\xi_i\rangle$ with the measurement of Definition 2.10, we get outcome 1 with probability at least $\frac{1}{16 \cdot 4^n}$. But this means that the Uniformity Test rejects with probability at least $\frac{1}{12 \cdot 16 \cdot 4^n} > \frac{1}{200 \cdot 4^n}$. This contradicts to the statement of the lemma, so it must be that $|\gamma_v^{(i)}|^2 \geq \frac{1}{2 \cdot 2^n}$ for all v . Lemma A.5 implies that for all v ,

$$|\alpha_v^{(i)}|^2 \geq \frac{1}{12 \cdot 2 \cdot 2^n}. \quad \square$$

We are now ready to prove soundness for V .

Lemma 4.5 (Soundness). *If $C_G \notin \text{SUCCINCT3COL}$ then V of Algorithm 2 will reject with probability at least $12000^{-1} \cdot 4^{-n}$.*

Proof. Suppose that the Uniformity Test rejects with probability at most $\frac{1}{200 \cdot 4^n}$, as otherwise we are done. From Lemma 4.3, $|Z'| > \frac{k}{6}$. Since $\frac{k}{6} = \Omega(n)$, we can always take $k \geq 12$ so we have $|Z'| > 2$. Let's pick two elements $q, r \in Z'$. We define two colorings c_1 and c_2 the following way,

$$c_1(v) \stackrel{\text{def}}{=} \arg \max_j \left| \beta_{v,j}^{(q)} \right|$$

and similarly

$$c_2(v) \stackrel{\text{def}}{=} \arg \max_j \left| \beta_{v,j}^{(r)} \right|,$$

for all $v \in \{0, 1, \dots, 2^n - 1\}$. If the maximum is not well defined then just choose an arbitrary j for which $\left| \beta_{v,j}^{(\cdot)} \right|$ is maximal. From Lemma 4.4 the probability that we get $(v, c_1(v))$ when we measure $|\phi_q\rangle$ in the standard basis is at least $\left| \alpha_v^{(q)} \right|^2 \cdot \frac{1}{3} > \frac{1}{72 \cdot 2^n}$, for all v , and the same lower-bound is true for getting $(v, c_2(v))$, when measuring $|\phi_r\rangle$. We split the rest of the proof into two cases.

- Suppose that the two colorings are different, i.e., $\exists v$ such that $c_1(v) \neq c_2(v)$. In this case in line 4 we get $(v, c_1(v))$ when measuring $N_q C_q$ and $(v, c_2(v))$ when measuring $N_r C_r$ with probability at least $\left(\frac{1}{72 \cdot 2^n} \right)^2 > \frac{1}{6000 \cdot 4^n}$. It means that with at least the above probability the Consistency Test will reject in line 8.
- Suppose that the two colorings are the same, i.e., $\forall v : c_1(v) = c_2(v)$. Since G is not 3-colorable, $\exists v_1, v_2 \in \{0, 1, \dots, 2^n - 1\}$ such that (v_1, v_2) is an edge in G and $c_1(v_1) = c_1(v_2)$, or equivalently $C_G(v_1, v_2) = 11$. Similarly as above, with probability at least $\frac{1}{6000 \cdot 4^n}$, we get $(v_1, c_1(v_1))$ when measuring $N_q C_q$ and $(v_2, c_1(v_2))$ when measuring $N_r C_r$ in line 4 of the algorithm. In this case the Consistency Test will reject with at least the above probability in line 10.

Since in both cases the Consistency Test rejects with probability at least $\frac{1}{6000 \cdot 4^n}$, and the test is chosen with probability $\frac{1}{2}$, the lemma follows. \square

Proof of Theorem 4.1. Note that Algorithm 2 runs in polynomial time. Furthermore, for both the Consistency and the Uniformity Test, the algorithm starts with measuring all the quantum registers according to a fixed measurement. So V is a proper BellQMA verifier. Lemma 4.2 shows that the completeness of the protocol is $c > 1 - 2^{-\frac{k}{40}}$, while Lemma 4.5 shows that the soundness is $s < 1 - 12000^{-1} \cdot 2^{-2n}$. If $k \geq 120n$ then $c - s = \Omega(2^{-2n})$ so the theorem follows. \square

5 Conclusions and Open Problems

In this section we discuss some of the consequences of the previous results, i.e., the consequences of Theorem 1.1 and 1.2. We also raise some related open problems.

5.1 Tightness of the Soundness Analyses

One can observe that both the QMA[2] verifier of Algorithm 1 and the BellQMA verifier of Algorithm 2 have soundness parameter $1 - \Omega(4^{-n})$ and gap $\Omega(4^{-n})$. (As shown by Lemma A.7 and Lemma 4.5.) Note that this bound is tight up to a constant factor in case of Algorithm 1 and tight up to some low-order term in case of Algorithm 2. The reason for this is the same as what was observed in one of the remark in [CF11].

The argument is briefly the following. Suppose that $C_G \notin \text{Succinct3Col}$ and that G is such, that there exist a coloring such that only one pair of nodes are colored inconsistently. If the prover gives

states of the form defined by equation (1) but using this coloring, then the verifier won't notice this in either of the Uniformity Tests nor in the Equality Test. The only place where the verifier can catch the prover is in the Consistency Test when it checks the colors of the nodes according to the constraints posed by the graph G . The prover gets caught if the verifier gets the inconsistently colored nodes in the measurement outputs. This happens with probability $O(2^{-2n})$ in case of Algorithm 1 and $O(n^2 2^{-2n})$ in case of Algorithm 2. This means that it is possible to fool the verifier of Algorithm 1 with probability $1 - O(4^{-n})$ and to fool the verifier of Algorithm 2 with probability $1 - \tilde{O}(4^{-n})$.

5.2 Separation Between QMA and QMA[2] in the Small-Gap Setting

As we said in the Introduction, it is a big open problem whether QMA is equal to QMA[2] or not, and we mentioned some evidences that suggest us that they are not equal. Here we give another evidence, i.e., we show that under plausible complexity-theoretic assumptions QMA[2] is *strictly* more powerful than QMA in the low-gap setting. We elaborate on this in the following.

Theorem 1.1 shows that QMA[2] with exponentially or double-exponentially small gap is exactly characterized by NEXP. So it is natural to ask, what is the power of QMA with the same gap, or what upper-bounds can we give for it? In a related paper, Ito et al. [IKW10] showed that quantum interactive proof systems (or the class QIP) with double-exponentially small gap are exactly characterized by EXP. Since QIP contains QMA with the same gap, we have a separation between QMA and QMA[2] in the setting where the gap is exponentially or double-exponentially small, unless $\text{EXP} = \text{NEXP}$. Note that the result of Ito et al. is quite involved. But if we are only interested in the upper-bound on QMA, then we can give a very simple argument for it, which we state and prove in the following lemma.

Lemma 5.1. $\bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(\text{poly}, 1, c, s) \subseteq \text{EXP}$, where $c(n)$ and $s(n)$ can be calculated in time at most exponential in n on a classical computer.

Proof sketch. Let x be an input to $\text{QMA}(\text{poly}, 1, c, s)$ with c and s having the above property. The action of the verifier can be described by a binary-valued measurement $\{\mathbf{P}_0^x, \mathbf{P}_1^x\}$ on the proof state, where \mathbf{P}_1^x corresponds to acceptance and \mathbf{P}_0^x corresponds to rejecting. Note that the maximum acceptance probability of the verifier is equal to the spectral norm of \mathbf{P}_1^x . (Or in other words the biggest eigenvalue of \mathbf{P}_1^x .) Since the proof is on poly-many qubits, the dimension of \mathbf{P}_1^x is exponential. An EXP-machine, knowing x , can approximate \mathbf{P}_1^x with up to an exponential amount of digits of accuracy. This is because the verifier is a uniform quantum circuit of polynomial size. Now the EXP-machine can approximate the spectral norm of \mathbf{P}_1^x up to an exponential amount of bits of accuracy. \square

5.2.1 One-Sided Error Case

Note that the NEXP characterization of the small-gap QMA[2] proof system still holds if we restrict the proof system to have one-sided error. Moreover, it is not known whether QMA can be made to have one-sided error, so we can investigate the relation between these classes as well. Interestingly, it turns out that we can state an even stronger separation in this case. This is due to a result by Ito et al. [IKW10].

Theorem 5.2 (Theorem 11 of [IKW10]). $\text{QMA}(\text{poly}, 1, 1, < 1) \subseteq \text{PSPACE}$.

This means that in the one-sided error case QMA[2] with exponentially small gap is *strictly* more powerful than QMA with even unbounded gap, unless $\text{PSPACE} = \text{NEXP}$!

5.3 Nonexistence of Disentanglers

The discussions in Section 5.2 have an interesting consequence to the existence question of certain operators called disentanglers. They were defined by Aaronson et al. [ABD⁺09], as the following.

Definition 5.3 (Definition 40 of [ABD⁺09]). Let us have a superoperator $\Phi : D(\mathbb{C}^N) \rightarrow D(\mathbb{C}^M \otimes \mathbb{C}^M)$.⁵ We say that Φ is an (ε, δ) -disentangler if

- $\Phi(\rho)$ is ε -close to a separable state for every ρ , and
- for every separable state σ , there exists a ρ such that $\Phi(\rho)$ is δ -close to σ .

Note that if there exist a $(\frac{1}{\text{poly}(\log M)}, \frac{1}{\text{poly}(\log M)})$ -disentangler with $\log N = \text{poly}(\log M)$, and if that disentangler can be implemented in $\text{poly}(\log M)$ -time, then $\text{QMA} = \text{QMA}[2]$. So it is not believed that such a disentangler exist. Towards proving this, Aaronson et al. showed that no $(0, 0)$ -disentangler exists for any finite N and M . The discussion in the previous section implies that there exist no disentangler with approximation error inverse of the square of the dimension. More precisely we have the following corollary.

Corollary 5.4. *There exist a function $f(M) = \Omega(M^{-2})$, such that there exist no $\text{poly}(\log M)$ -time implementable $(f(M), f(M))$ -disentangler with $\log N = \text{poly}(\log M)$, unless $\text{EXP} = \text{NEXP}$.*

Proof. Suppose that there exist such a disentangler Φ , for $f(M) = \kappa_1 \cdot M^{-2}$, for some constant κ_1 to be specified later. Let $L \in \text{NEXP}$. Theorem 3.2 implies that $L \in \text{QMA}(\text{poly}, 2, 1, 1 - \kappa_2 \cdot 4^{-n})$, for some constant κ_2 and where the dimension of both proof states are $3 \cdot 2^n$. Let V be the corresponding verifier. We show that $L \in \text{QMA}(\text{poly}, 1, c, s)$ with $c - s = \Omega(4^{-n})$ by constructing a verifier W that uses only one proof. By Lemma 5.1 it holds that $\text{QMA}(\text{poly}, 1, c, s) \subseteq \text{EXP}$ so we get that $\text{EXP} = \text{NEXP}$.

We are left to define verifier W . W first applies Φ on its quantum proof then simulates V on the output of Φ and outputs whatever V outputs. Note that Φ is poly -time implementable and the size of the proof of W is also polynomial. To see completeness for W , note that there exist a state $|\psi\rangle \otimes |\psi\rangle$ with which V accepts with probability 1. From Definition 5.3 there exist a ρ such that $\Phi(\rho)$ is $f(3 \cdot 2^n)$ -close to $|\psi\rangle \otimes |\psi\rangle$. Since $f(3 \cdot 2^n) = \frac{\kappa_1}{9} \cdot 4^{-n}$, the probability of acceptance of W is at least $1 - \frac{\kappa_1}{9} \cdot 4^{-n}$. Similarly, for the soundness of W , we have that for all separable states, V accepts with probability at most $1 - \kappa_2 \cdot 4^{-n}$. Again from Definition 5.3, for all ρ , $\Phi(\rho)$ is $f(3 \cdot 2^n)$ -close to a separable state. So the probability of acceptance of W is at most $1 - \kappa_2 \cdot 4^{-n} + \frac{\kappa_1}{9} \cdot 4^{-n}$. If κ_1 is sufficiently small then $c - s = \Omega(4^{-n})$, so the corollary follows. \square

5.4 Notes on BellQMA Proof Systems

An interesting consequence of Theorem 1.1 and 1.2 is that in the small-gap setting, $\text{BellQMA}[k]$ proof systems have the same power as $\text{QMA}[k]$ proof systems if k is at least a linear function of the input length. Such a result is not known to hold in the normal-gap setting. As we mentioned before, in the normal-gap setting we now that if k is constant then $\text{BellQMA}[k]$ collapses to QMA , and the proof of this fact doesn't generalize to the small-gap setting. This means that it is an interesting open question to figure out the power of $\text{BellQMA}[2]$ with exponentially small gap. There could be two possibilities:

- It is quite unlikely that the small-gap version of $\text{BellQMA}[2] = \text{NEXP}$, because it would give a very powerful proof system, and moreover it would show that if a verifier is restricted to Bell-measurements then it gains a lot of extra power if we decrease the bound on the gap; since $\text{BellQMA}[2] = \text{QMA}$ if the gap is inverse-polynomial, but $\text{BellQMA}[2] = \text{QMA}[2]$ if it is inverse-exponential.
- So we conjecture that the small-gap $\text{BellQMA}[2] \subset \text{NEXP}$. But this would imply that somewhere between constant and linear number of provers, the power of $\text{BellQMA}[k]$ significantly increases.

We leave the study of this class for future work.

⁵We denote the set of all density operators on space \mathcal{H} by $D(\mathcal{H})$.

5.5 Error and Proof Reduction

Note that as a side-product of our results, in both the BellQMA $[k]$ and QMA $[k]$ proof systems we can ‘amplify’ the error from double-exponentially small gap to single-exponentially small gap. Also in the case of QMA $[k]$, we can make the proof system to have *one-sided error*, which up to our knowledge, has only been shown to hold for QCMA [JKNN11]. (Additionally, the number of proofs can be reduced to two, but this also follows from [HM10], where an essentially different argument was used.)

5.6 QMA $[k]$ with Small Gap and Logarithmic-Length Proofs

We also examine multi-prover QMA proof systems with small gap and where each proof consist of at most $O(\log n)$ qubits, in the hope that we can separate them from the ones that have $\text{poly}(n)$ -length proofs. Unfortunately we were not able to do this in general, only in the case where the gap is inverse-exponential, which follows from a few simple observations. If the gap is smaller, say double-exponentially small or unbounded, then we give a lemma which simplifies the proof system by converting it to one with single-qubit proofs without changing the order of magnitude of the gap. The details follow.

Lemma 5.5. $\text{PP} = \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-\text{poly}}}} \text{QMA}(O(\log n), \text{poly}(n), c, s)$, where $c(n)$ and $s(n)$ can be calculated in $\text{poly}(n)$ -time on a classical computer.

Proof sketch. The containment $\text{PP} \subseteq \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-\text{poly}}}} \text{QMA}(O(\log n), \text{poly}(n), c, s)$ is trivial since in PP the gap is always at least inverse-exponential. So we only need to prove the other direction. Consider the class $\text{QMA}(O(\log n), \text{poly}(n), c, s)$ for some c and s , for which the conditions in the lemma hold. Note that $\text{QMA}(O(\log n), \text{poly}(n), c, s) \subseteq \text{QCMA}(c', s')$, where $c' - s' \geq 2^{-\text{poly}}$. (In fact they are equal.) The reason behind it is that for each proof there exists a unitary transformation that creates it, say, from $|0\rangle$. Since the unitaries are on $O(\log n)$ -many qubits, they can be described up to exponential precision by quantum circuits of size $\text{poly}(n)$. The QCMA verifier expects these descriptions as its proof. The completeness and soundness follows easily.⁶

The above QCMA proof system can be converted to an MA proof system with exponentially small gap in the following way. The MA proof is the same as the QCMA proof. Once the proof is fixed the question is to estimate the acceptance probability of a poly-time quantum computation to exponential precision. This problem is in PQP, and since $\text{PQP} = \text{PP}$,⁷ we have an MA proof system with the given parameters. This MA class is obviously in PP via the same argument as $\text{MA} \subseteq \text{PP}$ for the normal-gap version of MA. \square

Remark 5.6. Note that if we decrease the proof lengths to only 1 qubits then the resulting class is obviously still equals to PP. More formally

$$\text{PP} = \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-\text{poly}}}} \text{QMA}(1, \text{poly}(n), c, s),$$

where $c(n)$ and $s(n)$ can be calculated in $\text{poly}(n)$ -time on a classical computer.

This observation is generalized by the following lemma to any smaller gaps.

Lemma 5.7. $\text{QMA}(O(\log n), \text{poly}, c, s) \subseteq \text{QMA}(1, \text{poly}, 1 - 2^{-t} \cdot (1 - c), 1 - 2^{-t} \cdot (1 - s))$, for some t such that $t(n) \in \text{poly}(n)$, and c and s are arbitrary functions of n .

⁶For a detailed (but a bit different) proof of this fact see [GSU11].

⁷PQP is the unbounded-gap version of BQP. For the exact definition of the class and the proof of the above equality see for example the survey by Watrous [Wat08].

We present the proof of this lemma in Appendix B on page 19. Let us explicitly state here the previously mentioned corollary.

Corollary 5.8. *It holds that*

$$\bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(O(\log n), \text{poly}, c, s) = \bigcup_{\substack{0 < s < c \leq 1, \\ c-s \geq 2^{-2^{\text{poly}}}}} \text{QMA}(1, \text{poly}, c, s),$$

and

$$\bigcup_{0 < s < c \leq 1} \text{QMA}(O(\log n), \text{poly}, c, < s) = \bigcup_{0 < s < c \leq 1} \text{QMA}(1, \text{poly}, c, < s).$$

Note that in Lemma 5.7 the one-sided error property is preserved. So we also have for example

$$\text{QMA}(O(\log n), \text{poly}, 1, < 1) = \text{QMA}(1, \text{poly}, 1, < 1).$$

We don't know any better upper-bound for $\text{QMA}(1, \text{poly}, c, s)$ with $c - s \geq 2^{-2^{\text{poly}}}$ then the trivial NEXP. It would be interesting to strengthen this bound or give some non-trivial lower-bound. We leave this question for future work.

5.7 More Open Problems

Here we list some more open problems that we think may be interesting to work on.

- What is the power of $\text{QMA}[k]$ and $\text{BellQMA}[k]$ with unbounded gap? Can we at least show some upper-bounds?
- What is the power of $\text{QMA}\left(1, 1, 1, 1 - 2^{-2^{\text{poly}}}\right)$ or $\text{QMA}(1, 1, 1, < 1)$? I.e., the proof system has only one qubit as its proof but we allow double-exponentially small or unbounded gap. Are they the same as PQP? Note that the known $\text{QMA}\left(O(\log n), 1, \frac{2}{3}, \frac{1}{3}\right) = \text{BQP}$ proofs [MW05, BSW11] break down if the gap is so small.

Acknowledgements

The author would like to thank Rahul Jain and Penghui Yao for helpful discussions on the topic.

A Proof of Soundness for Theorem 3.2

This section proves soundness for verifier V described by Algorithm 1 on page 7; and hence finishes the proof of Theorem 3.2. The proof is done through a few lemmas.

From now on let us suppose that $C_G \notin \text{Succinct3COL}$, and let's denote the state of R_1 by $|\psi\rangle$, and the state of R_2 by $|\varphi\rangle$. These two states can be written in the form

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \sum_{j=0}^2 \beta_{i,j} |j\rangle, \quad |\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha'_i |i\rangle \sum_{j=0}^2 \beta'_{i,j} |j\rangle,$$

where $\sum_i |\alpha_i|^2 = \sum_i |\alpha'_i|^2 = 1$, and for all i , $\sum_j |\beta_{i,j}|^2 = \sum_j |\beta'_{i,j}|^2 = 1$.

The following lemma says that if the Equality Test succeeds with high probability then the distribution of outcomes in the Consistency Test will be similar. This is analogous to Lemma 2.5 of [BT09].

Lemma A.1. *If the Equality test of Algorithm 1 succeeds with probability at least $1 - \varepsilon$, then for all k and ℓ it holds that $\left| |\alpha_k \beta_{k,\ell}|^2 - |\alpha'_k \beta'_{k,\ell}|^2 \right| \leq \sqrt{8\varepsilon}$.*

Proof. Let $p_{i,j} = |\alpha_i \beta_{i,j}|^2$ and $q_{i,j} = |\alpha'_i \beta'_{i,j}|^2$, and let us denote the probability vector with elements $p_{i,j}$ by p , and similarly for q . Then we have the following.

$$\sqrt{1 - |\langle \psi | \varphi \rangle|^2} = \frac{1}{2} \| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \|_{\text{Tr}} \quad (2)$$

$$\geq \frac{1}{2} \|p - q\|_1 \quad (3)$$

$$= \frac{1}{2} \sum_{i,j} \left| |\alpha_i \beta_{i,j}|^2 - |\alpha'_i \beta'_{i,j}|^2 \right|$$

$$\geq \frac{1}{2} \left| |\alpha_k \beta_{k,\ell}|^2 - |\alpha'_k \beta'_{k,\ell}|^2 \right|,$$

for any k and ℓ . Equations (2) and (3) are from the properties of the trace distance. Theorem 2.9 implies that $\frac{1}{2} (1 + |\langle \psi | \varphi \rangle|^2) \geq 1 - \varepsilon$. With the above derivation the claim of the lemma follows. \square

Similarly to Lemma 2.6 of [BT09] (or Lemma 6.1 of [CF11]), the next lemma states that vertices with high probability of being observed have a well-defined color.

Lemma A.2. *Suppose that $|\psi\rangle$ and $|\varphi\rangle$ pass the Equality Test of Algorithm 1 and also line 9 in the Consistency Test with probability at least $1 - 10^{-10} \cdot 4^{-n}$. Then for all i for which $|\alpha_i|^2 \geq 100^{-1} \cdot 2^{-n}$, there exist one j for which $|\beta_{i,j}|^2 \geq 0.9$.*

Proof. Towards contradiction suppose that $\exists i$ such that $|\alpha_i|^2 \geq \frac{1}{100 \cdot 2^n}$ and $\forall j$ it holds that $|\beta_{i,j}|^2 < \frac{9}{10}$. Then without loss of generality we can say that $|\beta_{i,0}|^2 \geq \frac{1}{20}$ and $|\beta_{i,1}|^2 \geq \frac{1}{20}$. Since the probability that the Equality Test succeeds is at least $1 - \frac{1}{10^{10} \cdot 4^n}$, we can apply Lemma A.1 and get that

$$\left| |\alpha_i \beta_{i,1}|^2 - |\alpha'_i \beta'_{i,1}|^2 \right| \leq \frac{\sqrt{8}}{10^5 \cdot 2^n}.$$

This implies that

$$\begin{aligned} |\alpha'_i|^2 |\beta'_{i,1}|^2 &\geq |\alpha_i|^2 |\beta_{i,1}|^2 - \frac{\sqrt{8}}{10^5 \cdot 2^n} \\ &\geq \frac{1}{2000 \cdot 2^n} - \frac{\sqrt{8}}{10^5 \cdot 2^n}. \end{aligned}$$

Then the probability that in line 8 in the Consistency Test we get $v_1 = v_2 = i$, $c_1 = 0$ and $c_2 = 1$ is

$$\Pr[v_1 = i \text{ and } c_1 = 0] \cdot \Pr[v_2 = i \text{ and } c_2 = 1] \geq \frac{1}{2000 \cdot 2^n} \left(\frac{1}{2000 \cdot 2^n} - \frac{\sqrt{8}}{10^5 \cdot 2^n} \right) > \frac{1}{10^{10} \cdot 4^n}.$$

This contradicts to the assumption that $|\psi\rangle$ and $|\varphi\rangle$ pass line 9 with probability at least $1 - 10^{-10} \cdot 4^{-n}$. \square

The next lemma is analogous to Lemma 2.7 of [BT09] and also to Lemma 6.2 of [CF11].

Lemma A.3. *Suppose that $|\psi\rangle$ and $|\varphi\rangle$ pass the Equality Test of Algorithm 1 and also line 9 in the Consistency Test with probability at least $1 - 10^{-10} \cdot 4^{-n}$. Then the probability of measuring 0 on C_1 in line 17 in the Uniformity Test is at least 0.05.*

Proof. Suppose that we measure N_1 in the standard basis. If the outcome is i then the probability of measuring 0 on C_1 with the measurement of Definition 2.10 is

$$\frac{1}{3} |\beta_{i,0} + \beta_{i,1} + \beta_{i,2}|^2.$$

For all i for which $|\alpha_i|^2 \geq \frac{1}{100 \cdot 2^n}$ Lemma A.2 applies, which means that there exist k_i such that $|\beta_{i,k_i}|^2 \geq \frac{9}{10}$. Let $\ell_i \stackrel{\text{def}}{=} k_i + 1 \pmod{3}$ and $m_i \stackrel{\text{def}}{=} k_i + 2 \pmod{3}$; then $|\beta_{i,\ell_i}|^2 + |\beta_{i,m_i}|^2 < \frac{1}{10}$. We can lower bound the above probability by

$$\begin{aligned} \frac{1}{3} |\beta_{i,k_i} + \beta_{i,\ell_i} + \beta_{i,m_i}|^2 &\geq \frac{1}{3} ||\beta_{i,k_i}| - |\beta_{i,\ell_i} + \beta_{i,m_i}||^2 \\ &\geq \frac{1}{3} \left(|\beta_{i,k_i}| - \sqrt{2 \cdot (|\beta_{i,\ell_i}|^2 + |\beta_{i,m_i}|^2)} \right)^2 \\ &\geq \frac{1}{3} \left(\frac{9}{10} - \sqrt{\frac{2}{10}} \right)^2 \\ &> \frac{6}{100}, \end{aligned}$$

where the second inequality follows from the Cauchy–Schwarz inequality. Or more precisely we have $|\beta_{i,\ell_i} + \beta_{i,m_i}|^2 \leq 2 \cdot (|\beta_{i,\ell_i}|^2 + |\beta_{i,m_i}|^2) < \frac{2}{10} < \frac{9}{10} \leq |\beta_{i,k_i}|^2$. The probability of measuring 0 on C_1 in line 17 is

$$\begin{aligned} \sum_{i=0}^{2^n-1} |\alpha_i|^2 \cdot \frac{1}{3} \cdot |\beta_{i,0} + \beta_{i,1} + \beta_{i,2}|^2 &\geq \sum_{\substack{i \text{ for which} \\ |\alpha_i|^2 \geq \frac{1}{100 \cdot 2^n}}} |\alpha_i|^2 \cdot \frac{1}{3} \cdot |\beta_{i,0} + \beta_{i,1} + \beta_{i,2}|^2 \\ &> \frac{6}{100} \cdot \sum_{\substack{i \text{ for which} \\ |\alpha_i|^2 \geq \frac{1}{100 \cdot 2^n}}} |\alpha_i|^2 \\ &\geq \frac{6}{100} \cdot \left(1 - \frac{2^n - 1}{100 \cdot 2^n} \right) \\ &> \frac{5}{100}, \end{aligned}$$

where we used the fact that at most $2^n - 1$ nodes (i 's) can have $|\alpha_i|^2 < \frac{1}{100 \cdot 2^n}$. □

In order to proceed we need two lemmas, one from [BT09] and one from [CD10]. We present them now, together with their proofs.

Lemma A.4 (Lemma 2.8 of [BT09]). *Let us have a state $|\xi\rangle \in \mathbb{C}^m$, $|\xi\rangle = \sum_{i=0}^{m-1} \gamma_i |i\rangle$. If there exist a k such that $|\gamma_k|^2 < \frac{1}{2m}$, then the probability of getting 1 when we measure $|\xi\rangle$ with the measurement of Definition 2.10 is at least $\frac{1}{16m^2}$.*

Proof. Let p and q be the probability distributions that arise when we measure $|\xi\rangle$ and $|u_m\rangle$ in the computational basis. Or in other words, let p be the probability vector with elements $|\gamma_i|^2$, and q be the

vector with all elements equal to $\frac{1}{m}$. Similarly to Lemma A.1 we have that

$$\begin{aligned}
\sqrt{1 - |\langle u_m | \xi \rangle|^2} &= \frac{1}{2} \| |u_m\rangle \langle u_m| - |\xi\rangle \langle \xi| \|_{\text{Tr}} \\
&\geq \frac{1}{2} \|q - p\|_1 \\
&= \frac{1}{2} \sum_{i=0}^{m-1} \left| \frac{1}{m} - |\gamma_i|^2 \right| \\
&\geq \frac{1}{2} \left| \frac{1}{m} - |\gamma_k|^2 \right| \\
&> \frac{1}{4m}.
\end{aligned}$$

Since the probability of getting 1 when we measure $|\xi\rangle$ with the measurement of Definition 2.10 is $1 - |\langle u_m | \xi \rangle|^2$, the statement of the lemma follows. \square

The following argument appears in the proof of Lemma 3 of [CD10], which we state here as a separate lemma.

Lemma A.5. *Suppose that we have a bipartite quantum state $|\psi\rangle \in \mathcal{N} \otimes \mathcal{C}$, with $\mathcal{N} = \mathbb{C}^N$ and $\mathcal{C} = \mathbb{C}^C$. We can write this state as*

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle \sum_{j=0}^{C-1} \beta_{i,j} |j\rangle,$$

where $\sum_i |\alpha_i|^2 = 1$, and for all i , $\sum_j |\beta_{i,j}|^2 = 1$. Suppose that the probability of measuring 0 on \mathcal{C} with the measurement of Definition 2.10 is p , and after the measurement the resulting state on \mathcal{N} is

$$|\xi\rangle \in \mathcal{N}, \quad |\xi\rangle = \sum_{i=0}^{N-1} \gamma_i |i\rangle,$$

with $\sum_i |\gamma_i|^2 = 1$. Then for all i it holds that

$$|\alpha_i|^2 \geq p \cdot |\gamma_i|^2.$$

Proof. Let q_i denote the probability that if we measure the \mathcal{C} part of $|\psi\rangle$ with the measurement of Definition 2.10 we get outcome 0, then if we measure the \mathcal{N} part in the standard basis, we get i . Note that for all i ,

$$q_i = p \cdot |\gamma_i|^2.$$

On the other hand,

$$\begin{aligned}
q_i &= \langle \psi | (|i\rangle \langle i| \otimes |u_C\rangle \langle u_C|) | \psi \rangle \\
&= \frac{|\alpha_i|^2}{C} \cdot \left| \sum_{j=0}^{C-1} \beta_{i,j} \right|^2 \\
&\leq \frac{|\alpha_i|^2}{C} \cdot C \cdot \sum_{j=0}^{C-1} |\beta_{i,j}|^2 \\
&= |\alpha_i|^2,
\end{aligned}$$

where the inequality above follows from the Cauchy–Schwarz inequality. The above derivations imply the statement of the lemma. \square

Analogously to Lemma 2.9 of [BT09] (and to Lemma 6.3 of [CF11]), the following lemma says that if the states pass some of the tests with high probability, then it must be that all nodes appear with high enough probability.

Lemma A.6. *Suppose that $|\psi\rangle$ and $|\phi\rangle$ pass the Equality Test of Algorithm 1, line 9 in the Consistency Test, and also the Uniformity Test with probability at least $1 - 10^{-10} \cdot 4^{-n}$. Then for all i , $|\alpha_i|^2 \geq 100^{-1} \cdot 2^{-n}$.*

Proof. Because of Lemma A.3 the probability of measuring 0 on C_1 in line 17 of Algorithm 1 is at least $\frac{5}{100}$. Let the state of N_1 be $|\xi\rangle = \sum_{i=0}^{2^n-1} \gamma_i |i\rangle$, after we got 0 on C_1 . Towards contradiction suppose that $\exists i$ such that $|\alpha_i|^2 < \frac{1}{100 \cdot 2^n}$. Since we got this measurement result with probability $\geq \frac{5}{100}$, Lemma A.5 implies that $|\gamma_i|^2 < \frac{1}{5 \cdot 2^n}$. From Lemma A.4 the probability of getting 1 when measuring N_1 in line 17 is at least $\frac{1}{16 \cdot 4^n}$. So the probability of failing the Uniformity Test is at least $\frac{5}{100} \cdot \frac{1}{16 \cdot 4^n} > \frac{1}{10^{10} \cdot 4^n}$. This is a contradiction. \square

The following lemma finishes the proof of soundness for verifier V .

Lemma A.7 (Soundness). *If $C_G \notin \text{SUCCINCT3COL}$ then verifier V described by Algorithm 1 will reject with probability at least $\frac{1}{3 \cdot 10^{10} \cdot 4^n}$.*

Proof. Assume that $|\psi\rangle$ and $|\phi\rangle$ pass the Equality Test, the Uniformity Test, and line 9 of Algorithm 1 with probability at least $1 - \frac{1}{10^{10} \cdot 4^n}$, as otherwise we are done. Let $c(i)$ be equal to the j for which $|\beta_{i,j}|$ is maximal, or in other words,

$$c(i) \stackrel{\text{def}}{=} \arg \max_j |\beta_{i,j}|.$$

Because of Lemma A.6 and A.2 this maximum is well defined. According to Lemma A.6, when measuring $|\psi\rangle$ in line 8, the probability of obtaining $(k, c(k))$, for all k , is at least $|\alpha_k|^2 \cdot \frac{9}{10} \geq \frac{1}{100 \cdot 2^n} \cdot \frac{9}{10} > \frac{1}{120 \cdot 2^n}$. Similarly, from Lemma A.1, for all k the probability that we get $(k, c(k))$ when measuring $|\phi\rangle$ in line 8, is at least $\frac{1}{120 \cdot 2^n} - \frac{\sqrt{8}}{10^5 \cdot 2^n} > \frac{1}{240 \cdot 2^n}$. Since the graph is not 3-colorable $\exists u, v \in V$ such that $(u, v) \in E$ and $c(u) = c(v)$. If in line 8 we get $(u, c(u))$ and $(v, c(v))$ then the Consistency Test will reject. This happens with probability at least

$$\frac{1}{120 \cdot 2^n} \cdot \frac{1}{240 \cdot 2^n} > \frac{1}{10^{10} \cdot 4^n}.$$

Since the Consistency Test is chosen with probability $\frac{1}{3}$, the statement of the lemma follows. \square

B Proof of Lemma 5.7

This section presents the proof of Lemma 5.7 from page 14. We will need the following previously known facts.

Lemma B.1 (See e.g., Chapter 4.5.2 of [NC00]). *An arbitrary unitary operator on m qubits can be implemented using a circuit containing $O(m^2 4^m)$ single-qubit and **CNOT** gates.*

Lemma B.2. *Any two-dimensional unitary operator U can be written in the form*

$$U = e^{i\theta} \mathbf{R}_z(\alpha) \mathbf{H} \mathbf{R}_z(\beta) \mathbf{H} \mathbf{R}_z(\gamma),$$

for $\alpha, \beta, \gamma, \theta \in [0, 2\pi)$.

Proof. It is well-known that one can write any U as $U = e^{i\vartheta} \mathbf{R}_z(\alpha) \mathbf{R}_x(\beta) \mathbf{R}_z(\gamma)$.⁸ The lemma follows from the fact that $\mathbf{R}_x(\beta) = e^{i\frac{\pi}{4}} \mathbf{H} \mathbf{R}_z(\beta) \mathbf{H}$. \square

⁸See e.g., Theorem 4.1 and Exercise 4.11 from [NC00].

The following definition and lemma are from [BK05], but we restate them in a different way, and include the proof for the sake of completeness.

Definition B.3. Define the ‘magic’ state $|m_\omega\rangle$ to be $|m_\omega\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\omega}|1\rangle)$.

Lemma B.4. *There exists a constant size quantum circuit, made up of **H**, **CNOT** and classical logical gates, such that on input $|\varphi\rangle$ and $|m_\omega\rangle$, it produces the state $\mathbf{R}_z(\omega)|\varphi\rangle$ with probability $1/2$. (This probability is independent of $|\varphi\rangle$ and ω .)*

Proof. Let $|\varphi\rangle = a|0\rangle + b|1\rangle$ for some $a, b \in \mathbb{C}$, with $|a|^2 + |b|^2 = 1$. On input $|m_\omega\rangle \otimes |\varphi\rangle$ the circuit performs the projective measurement defined by projectors

$$\mathbf{P}_1 = |00\rangle\langle 00| + |11\rangle\langle 11|, \quad \mathbf{P}_2 = |01\rangle\langle 01| + |10\rangle\langle 10|.$$

Note that

$$\begin{aligned} \mathbf{P}_1(|m_\omega\rangle \otimes |\varphi\rangle) &= \frac{1}{\sqrt{2}}(a|00\rangle + e^{i\omega}b|11\rangle), \text{ and} \\ \mathbf{P}_2(|m_\omega\rangle \otimes |\varphi\rangle) &= \frac{1}{\sqrt{2}}(b|01\rangle + e^{i\omega}a|10\rangle). \end{aligned}$$

This means that both measurement outcomes happen with probability $1/2$. If the outcome is 2, the circuit fails to create the state. However, if the measurement outcome is 1, then it performs a **CNOT**, which disentangles the second qubit, and gets the state

$$a|0\rangle + e^{i\omega}b|1\rangle = \mathbf{R}_z(\omega)|\varphi\rangle. \quad \square$$

By combining the lemmas above we get the following corollary.

Corollary B.5. *Let \mathbf{U} be any unitary operator on m qubits. There exist an algorithm A , using **H**, **CNOT** and classical logical gates, that takes as input the classical description of the circuit representing \mathbf{U} (as in Lemma B.1 and B.2) and the unentangled magic states (as in Lemma B.4), and produce the state $\mathbf{U}|0\rangle$, with probability $2^{-O(m^2 4^m)}$. Both the length of the input and the running time of A is $O(m^2 4^m)$.*

We are ready to prove Lemma 5.7.

Proof of Lemma 5.7. Let $L \in \text{QMA}(\ell, k, c, s)$, where $\ell \in O(\log n)$ and $k \in \text{poly}(n)$. (As usual, n is the length of the input.) Without loss of generality assume that all the proofs have length ℓ . Let V be the corresponding verifier. We now construct a proof system that recognizes the same language L , and all the proofs are 1 qubit long.

Denote the new verifier by W . For its proofs, W expects to get the circuit descriptions of k unitary operators $\mathbf{U}_1, \dots, \mathbf{U}_k$, together with the corresponding unentangled 1 qubit magic states. Let us denote the number of magic states by t . Since each \mathbf{U}_i lives on ℓ qubits, the total number of bits and qubits W gets from the provers are at most $O(k \cdot \ell^2 4^\ell) \in \text{poly}(n)$. W uses algorithm A from Corollary B.5, k times, to get the states $\mathbf{U}_1|0\rangle, \dots, \mathbf{U}_k|0\rangle$. If in any of these k cases A fails then W accepts. Otherwise W runs V on $\mathbf{U}_1|0\rangle \otimes \dots \otimes \mathbf{U}_k|0\rangle$ and accepts if and only if V accepts. The running time of W is obviously polynomial. Let us denote the probability of acceptance of V on input $\mathbf{U}_1|0\rangle \otimes \dots \otimes \mathbf{U}_k|0\rangle$ by p . There are two cases for W .

- With probability $1 - 2^{-t}$ one of the runs of algorithm A fails and W accepts.
- With probability 2^{-t} all the A s succeed. In this case W obtains the state $\mathbf{U}_1|0\rangle \otimes \dots \otimes \mathbf{U}_k|0\rangle$. Given this state as input to V , it accepts with probability p .

The overall probability with which W accepts is

$$1 - 2^{-t} + 2^{-t}p = 1 - 2^{-t}(1 - p).$$

We are left to argue about completeness and soundness. For the completeness assume that there exist states $|\phi_1\rangle, \dots, |\phi_k\rangle$, with which V accepts with probability at least c . Then there exists unitary operators U'_1, \dots, U'_k such that $|\phi_i\rangle = U'_i|0\rangle$ for $i \in \{1, 2, \dots, k\}$. The honest provers of W can give the descriptions of these unitaries together with the corresponding magic states, so the completeness parameter follows. For the soundness assume that for all states $|\phi_1\rangle, \dots, |\phi_k\rangle$, V accepts with probability at most s . Then even if W gets arbitrary circuit descriptions and magic states, they correspond to some unitaries when all the runs of A succeed. So the soundness follows similarly to the completeness. \square

References

- [AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.
- [ABD⁺09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009, arXiv:0804.0802.
- [AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey. 2002, arXiv:quant-ph/0210077.
- [Ba08] Fernando G. S. L. Brandão. *Entanglement Theory and the Quantum Simulation of Many-Body Physics*. PhD thesis, Imperial College London, 2008, arXiv:0810.0026.
- [Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the 17th annual ACM Symposium on Theory of Computing*, STOC '85, pages 421–429, 1985.
- [BaCY11] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. A quasipolynomial-time algorithm for the quantum separability problem. In *Proceedings of the 43rd annual ACM Symposium on Theory of Computing*, STOC '11, pages 343–352, 2011, arXiv:1011.2751.
- [BAD⁺97] Adriano Barenco, Berthiaume André, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM J. Comput.*, 26:1541–1557, October 1997, arXiv:quant-ph/9604028.
- [BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, Sep 2001, arXiv:quant-ph/0102001.
- [Bei10] Salman Beigi. NP vs QMA_{log}(2). *Quantum Info. Comput.*, 10(1):141–151, January 2010, arXiv:0810.5109.
- [BK05] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, Feb 2005, arXiv:quant-ph/0403025.
- [BSW11] Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7(1):101–117, 2011, arXiv:1004.0411.
- [BT09] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *Third International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009, arXiv:0709.0738.

- [CD10] Jing Chen and Andrew Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. November 2010, arXiv:1011.0716.
- [CF11] Alessandro Chiesa and Michael Forbes. Improved soundness for QMA with multiple provers. August 2011, arXiv:1108.2098.
- [GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.
- [GNN11] François Le Gall, Shota Nakagawa, and Harumichi Nishimura. On QMA protocols with two short quantum proofs. August 2011, arXiv:1108.4306.
- [GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th annual ACM Symposium on Theory of Computing*, STOC '86, pages 59–68, 1986.
- [GSU11] Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. August 2011, arXiv:1108.0617.
- [GW83] Hana Galperin and Avi Wigderson. Succinct representations of graphs. *Information and Control*, 56(3):183–198, 1983.
- [HM10] Aram W. Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum Merlin-Arthur games. In *51st Annual IEEE Symposium on Foundations of Computer Science*, pages 633–642, 2010, arXiv:1001.0017.
- [IKW10] Tsuyoshi Ito, Hirotada Kobayashi, and John Watrous. Quantum interactive proofs with weak error bounds. December 2010, arXiv:1012.4427.
- [JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. In *Proceedings of the 42nd annual ACM Symposium on Theory of Computing*, STOC '10, pages 573–582, 2010, arXiv:0907.4737.
- [JKNN11] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. November 2011, arXiv:1111.5306.
- [KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer Berlin / Heidelberg, 2003, arXiv:quant-ph/0306051.
- [Kni96] Emanuel Knill. Quantum randomness and nondeterminism. 1996, arXiv:quant-ph/9610012.
- [KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.
- [KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd annual ACM Symposium on Theory of Computing*, STOC '00, pages 608–617, 2000.
- [LCV07] Yi-Kai Liu, Matthias Christandl, and F. Verstraete. Quantum computational complexity of the N -representability problem: QMA complete. *Phys. Rev. Lett.*, 98:110503, Mar 2007.

- [LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, October 1992.
- [MW05] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14:122–152, 2005, arXiv:cs/0506068.
- [NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [Per11] Attila Pereszlényi. On quantum interactive proofs with short messages. September 2011, arXiv:1109.0964.
- [PY86] Christos H. Papadimitriou and Mihalis Yannakakis. A note on succinct representations of graphs. *Information and Control*, 71(3):181–185, 1986.
- [Sha92] Adi Shamir. $IP = PSPACE$. *J. ACM*, 39(4):869–877, October 1992.
- [Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual IEEE Symposium on Foundations of Computer Science*, pages 537–546, 2000, arXiv:cs/0009002.
- [Wat03] John Watrous. $PSPACE$ has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.
- [Wat08] John Watrous. Quantum computational complexity. April 2008, arXiv:0804.3401.